COVID-19 PHISHING SCAMS

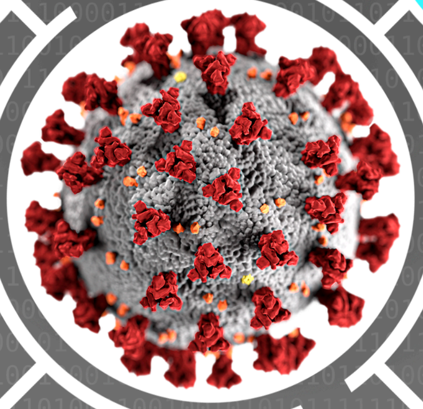
The coronavirus pandemic has resulted in a spike in misinformation and scamming opportunities. Email security firm Proofpoint reported that 80% of emails intercepted had something to do with the pandemic, while cloud-based email management company Mimecast reported detecting three million COVID-19 emails daily, the vast majority of which was believed to be malicious. The World Health Organization has reported criminals sending fraudulent WHO emails, and Kaspersky Labs has reported fraudulent CDC emails.

In anticipating a continued increase in fraudulent coronavirus attempts, consider the following suggestions to keep you and your organization safe.

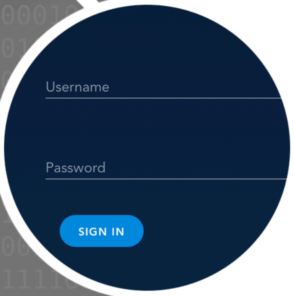
Do not provide personal information in response to any online request
Avoid clicking on suspicious email links

You are at risk
Know attackers are out there ready to scam you out of information and/or money

Verify websites are legitimate
Websites asking for information should have a padlock image next to the address signifying a secure connection



Avoid disinformation
Obtain and cross-check information from reputable sources; be wary of information posted on social media



Create unique usernames and passwords for each account
This reduces the risk of extensive compromise across multiple accounts

UTAH COUNTIES
INDEMNITY POOL